

[illegible]

10

15

20

25

an encryption apparatus, comprising:
means for encrypting a data body; and
means for transmitting transmission data to
a receiver, the transmission data including:

the encrypted data body;

sender's key recovery data obtained by encrypting
recovery information for recovering a key for
decrypting the encrypted data body to allow a key
recovery agent registered by a sender to decrypt
the recovery information; and

receiver's key recovery data obtained by
encrypting the recovery information for recovering
the key for decrypting the encrypted data body to
allow a key recovery agent registered by a receiver
to decrypt the recovery information; and

a plurality of key recovery agents each, when
registered by sender or receiver, capable of decrypting
sender's or receiver's key comprised of a plurality of
key pieces obtained by dividing the key into pieces.

4. A cryptographic communication system according
to claim 3, further comprising:

a certificate authority apparatus arranged
to allow accepting registration of at least key
recovery agent and receivers and provide information
representing correspondence between each registered
receiver and a key recovery agent and information
representing that said encryption apparatus encrypts

the recovery information so as to allow the key recovery agent to decrypt the recovery information.

5. A cryptographic communication system according to claim 3, further comprising:

an approver apparatus for approving a requester for key recovery agent registration approval and approving an authorized third party, who requests an approval for decrypting the sender's or receiver's key recovery data, to decrypt the sender's or receiver's key recovery data; and

wherein said key decrypter apparatus decrypts and sends back the sender's or receiver's key recovery data only when a request is made by a party approved by an approver.

6. A cryptographic communication system according to claim 4, further comprising:

an approver apparatus for approving a requester for key recovery agent registration approval and approving an authorized third party, who requests an approval for decrypting the sender's or receiver's key recovery data, to decrypt the sender's or receiver's key recovery data; and

wherein said key decrypter apparatus decrypts and sends back the sender's or receiver's key recovery data only when a request is made by a party approved by an approver.

7. A key recovery system comprising:

an encryption apparatus using key information for encrypting or decrypting data and storing, independently of key information, recovery information for recovering key information in an encrypted state so as to be decrypted by a key recovery agent registered by said encryption apparatus;

an approver apparatus for approving a party who requests a registration approval for the key recovery agent and giving an authorized party who requests an approval for decrypting the encrypted recovery information an approval for decrypting the encrypted recovery information; and

a key decrypter apparatus for decrypting and sending back the encrypted recovery information only when a decryption request is made by a party approved by an approver.

8. A computer-readable storage medium storing a program for controlling an encryption apparatus for encrypting a data body to make an encrypted data body contain in transmission data and transmitting the transmission data to a receiver, said program comprising means for containing, in the transmission data;

sender's key recovery data obtained by encrypting recovery information for recovering a key for decrypting the encrypted data body to allow a key recovery agent registered by a sender to decrypt

the recovery information; and

receiver's key recovery data obtained by
encrypting the recovery information for recovering
the key for decrypting the encrypted data body to
allow a key recovery agent registered by a receiver
to decrypt the recovery information.

5

CONFIDENTIAL